

PCT COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

Commissioner
 US Department of Commerce
 United States Patent and Trademark
 Office, PCT
 2011 South Clark Place Room
 CP2/5C24
 Arlington, VA 22202
 ETATS-UNIS D'AMERIQUE
 in its capacity as elected Office

Date of mailing (day/month/year) 29 May 2001 (29.05.01)	Applicant's or agent's file reference K 51 755/7ch
International application No. PCT/EP00/09131	Priority date (day/month/year) 20 September 1999 (20.09.99)
International filing date (day/month/year) 18 September 2000 (18.09.00)	
Applicant BALDISCHWEILER, Michael	

1. The designated Office is hereby notified of its election made:

☒ in the demand filed with the International Preliminary Examining Authority on:
 07 March 2001 (07.03.01)

☐ in a notice effecting later election filed with the International Bureau on:

2. The election ☒ was
☐ was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland Facsimile No.: (41-22) 740.14.35	Authorized officer Claudio Borton Telephone No.: (41-22) 338.83.38
------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

(Artikel 36 und Regel 70 PCT)

REC'D 24 JAN 2002

WIPO PCT


Aktenzeichen des Anmelders oder Anwalts K 51 755/7 so	WEITERES VORGEHEN siehe Mitteilung über die Übersendung des internationalen vorläufigen Prüfungsberichts (Formblatt PCT/IPEA/416)	
Internationales Aktenzeichen PCT/EP00/09131	Internationales Anmeldedatum (Tag/Monat/Jahr) 18/09/2000	Prioritätsdatum (Tag/Monat/Jahr) 20/09/1999
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G06F11/00		
Anmelder GIESECKE & DEVRIENT GMBH et al.		

- Dieser internationale vorläufige Prüfungsbericht wurde von der mit der internationalen vorläufigen Prüfung beauftragten Behörde erstellt und wird dem Anmelder gemäß Artikel 36 übermittelt.
- Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.
 - ☐ Außerdem liegen dem Bericht ANLAGEN bei; dabei handelt es sich um Blätter mit Beschreibungen, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit vor dieser Behörde vorgenommenen Berichtigungen (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsrichtlinien zum PCT).

Diese Anlagen umfassen insgesamt 3 Blätter.

3. Dieser Bericht enthält Angaben zu folgenden Punkten:

- I ☒ Grundlage des Berichts
- II ☐ Priorität
- III ☐ Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit
- IV ☒ Mangelnde Einheitlichkeit der Erfindung
- V ☒ Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung
- VI ☐ Bestimmte angeführte Unterlagen
- VII ☐ Bestimmte Mängel der internationalen Anmeldung
- VIII ☐ Bestimmte Bemerkungen zur internationalen Anmeldung

Datum der Einreichung des Antrags 07/03/2001	Datum der Fertigstellung dieses Berichts 22.01.2002
Name und Postanschrift der mit der internationalen vorläufigen Prüfung beauftragten Behörde:  Europäisches Patentamt D-80298 München Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Bevollmächtigter Bediensteter Bozas, I Tel. Nr. +49 89 2399 7408



I. Grundlage des Berichts

1. Hinsichtlich der **Bestandteile** der internationalen Anmeldung (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt, weil sie keine Änderungen enthalten (Regeln 70.16 und 70.17)*):
Beschreibung, Seiten:

1-7 ursprüngliche Fassung

1a eingegangen am 26/11/2001 mit Schreiben vom 26/11/2001

Patentansprüche, Nr.:

1-5 eingegangen am 26/11/2001 mit Schreiben vom 26/11/2001

Zeichnungen, Blätter:

1/2,2/2 ursprüngliche Fassung

2. Hinsichtlich der **Sprache**: Alle vorstehend genannten Bestandteile standen der Behörde in der Sprache, in der die internationale Anmeldung eingereicht worden ist, zur Verfügung oder wurden in dieser eingereicht, sofern unter diesem Punkt nichts anderes angegeben ist.

Die Bestandteile standen der Behörde in der Sprache: zur Verfügung bzw. wurden in dieser Sprache eingereicht; dabei handelt es sich um

- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen Recherche eingereicht worden ist (nach Regel 23.1(b)).
- ☐ die Veröffentlichungssprache der internationalen Anmeldung (nach Regel 48.3(b)).
- ☐ die Sprache der Übersetzung, die für die Zwecke der internationalen vorläufigen Prüfung eingereicht worden ist (nach Regel 55.2 und/oder 55.3).

3. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale vorläufige Prüfung auf der Grundlage des Sequenzprotokolls durchgeführt worden, das:

- ☐ in der internationalen Anmeldung in schriftlicher Form enthalten ist.
- ☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.
- ☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.
- ☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.
- ☐ Die Erklärung, daß die in computerlesbarer Form erfassten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

4. Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung, Seiten:
- ☐ Ansprüche, Nr.:
- ☐ Zeichnungen, Blatt:

5. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der Änderungen erstellt worden, da diese aus den angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2(c)).

(Auf Ersatzblätter, die solche Änderungen enthalten, ist unter Punkt 1 hinzuweisen; sie sind diesem Bericht beizufügen).

6. Etwaige zusätzliche Bemerkungen:

IV. Mangelnde Einheitlichkeit der Erfindung

1. Auf die Aufforderung zur Einschränkung der Ansprüche oder zur Zahlung zusätzlicher Gebühren hat der Anmelder:

- ☐ die Ansprüche eingeschränkt.
- ☐ zusätzliche Gebühren entrichtet.
- ☐ zusätzliche Gebühren unter Widerspruch entrichtet.
- ☐ weder die Ansprüche eingeschränkt noch zusätzliche Gebühren entrichtet.

2. ☒ Die Behörde hat festgestellt, daß das Erfordernis der Einheitlichkeit der Erfindung nicht erfüllt ist, und hat gemäß Regel 68.1 beschlossen, den Anmelder nicht zur Einschränkung der Ansprüche oder zur Zahlung zusätzlicher Gebühren aufzufordern.

3. Die Behörde ist der Auffassung, daß das Erfordernis der Einheitlichkeit der Erfindung nach den Regeln 13.1, 13.2 und 13.3

- ☐ erfüllt ist
- ☒ aus folgenden Gründen nicht erfüllt ist:
siehe Beiblatt

4. Daher wurde zur Erstellung dieses Berichts eine internationale vorläufige Prüfung für folgende Teile der internationalen Anmeldung durchgeführt:

- ☒ alle Teile.
- ☐ die Teile, die sich auf die Ansprüche Nr. beziehen.

INTERNATIONALER VORLÄUFIGER PRÜFUNGSBERICHT

Internationales Aktenzeichen PCT/EP00/09131

V. Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Feststellung

Neuheit (N)	Ja: Ansprüche	1-5
	Nein: Ansprüche	
Erfinderische Tätigkeit (ET)	Ja: Ansprüche	1, 3-4
	Nein: Ansprüche	2, 4-5
Gewerbliche Anwendbarkeit (GA)	Ja: Ansprüche	1-5
	Nein: Ansprüche	

2. Unterlagen und Erklärungen siehe Beiblatt

Zu Punkt IV

Mangelnde Einheitlichkeit der Erfindung

1. Es wird auf folgende Dokumente verwiesen:

D1: US-A-5 651 111

D2: US-A-5 715 389

D3: US-A-5 761 414

2. Die internationale Anmeldung erfüllt aus folgenden Gründen nicht die in Regel 30 PCT genannten Erfordernisse bezüglich Einheitlichkeit:

Die gemeinsamen Merkmale der unabhängigen Ansprüche 1 und 2 sind folgende:

Verfahren zur Sicherung des Programablaufs beim Aufruf von Unterprogrammen, wobei das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt.

Dokument D1 offenbart alle gemeinsamen Merkmale der unabhängigen Ansprüche 1 und 2 (siehe D1, Zusammenfassung; Spalte 14, Zeilen 17-20 und 33-63; Spalte 15, Zeilen 17-57; Anspruch 20).

Obwohl das in D1 beschriebene Verfahren zum Erzeugen eines Software-Testsystems entwickelt worden ist, ist es durchaus auch geeignet zur Überprüfung der Daten, die einem aufgerufenen Program übergeben werden, wobei die Überprüfung von dem aufgerufenen Program selbst erfolgt (siehe PCT Richtlinien, Teil C, Kapitel III-4.8).

Folglich sind die gemeinsamen Merkmale der unabhängigen Ansprüche 1 und 2 nicht neu. Die erforderliche Einheitlichkeit der Erfindung (Regel 13.1 PCT) ist damit insofern nicht mehr gegeben, als zwischen den Gegenständen der unabhängigen Ansprüche 1 und 2 kein technischer Zusammenhang im Sinne der Regel 13.2 PCT besteht, der in einem oder mehreren gleichen oder entsprechenden besonderen technischen Merkmalen zum Ausdruck kommt.

Zu Punkt V

Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung

1. Erste Gruppe: Ansprüche 1, 3-4

Aufgabe der Erfindung ist es, ein Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen bereitzustellen, wobei der Programmablauf von unerlaubten Manipulationen zu schützen ist. Diese Aufgabe wird durch das in dem unabhängigen Anspruch 1 beschriebene Verfahren gelöst. Das Verfahren verhindert eine unerlaubte Manipulation, in dem es verlangt, daß ein aufgerufenes Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt. Die Überprüfung erfolgt mittels einer Checksumme. Insbesondere, werden Checksummen über die zu übergebenden Parameter vor und nach der Übergabe gebildet und miteinander verglichen. Eine Ungleichheit der beiden Checksummen führt zum Abbruch des Programms bzw. zu einer Fehlermeldung.

Dokument D1, das den nächstliegenden Stand der Technik für den Anspruch 1 repräsentiert, beschreibt ein Testverfahren, das bei der Softwareentwicklung eingesetzt wird um das Testen von Softwaremodulen zu automatisieren. Obwohl, das in D1 beschriebene Verfahren eine Überprüfung der unter verschiedenen Routinen übergebenen Parameter erwähnt, unterscheidet sich der Offenbarungsgehalt des Dokuments D1 vom Gegenstand des Anspruchs 1, dadurch, daß die vorgenommene Überprüfung nicht mittels gebildeten Checksummen erfolgt. D1 gibt auch keinen Hinweis in der Richtung, weil es sich mit einem anderen Problem befaßt (Software-testing, Debugging, formale Parameterüberprüfung) als die Anmeldung (Sicherheit des Programmablaufs).

2. Zweite Gruppe: Ansprüche 2, 4-5

2.1 Erfinderische Tätigkeit, Artikel 33(3) PCT:

Die Anmeldung erfüllt aus folgenden Gründen nicht das in Artikel 33(3) PCT genannte Kriterium bezüglich erfinderischer Tätigkeit:

Anspruch 2:

Dokument D3, das als nächstliegender Stand der Technik für Anspruch 2 angesehen wird, offenbart ein Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen (Zusammenfassung), dadurch gekennzeichnet, daß bei Aufruf eines Unterprogramms ein Timer gestartet wird (Zusammenfassung; Figur 1a; Spalte 2, Zeilen 17-21), welcher die für die Ausführung des Programms benötigte Anzahl von Taktzyklen zählt und das Programm abbricht, wenn vor Beendigung des Unterprogramms die vorgegebene Anzahl der Taktzyklen überschritten wurde (Zusammenfassung).

Demgemäß unterscheidet sich der Gegenstand des unabhängigen Anspruchs 2 von dem Verfahren in D3, in dem das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt .

Dieses Merkmal repräsentiert einen allgemeinen und aus dem Stand der Technik bekannten Verfahrensschritt (siehe z.B. D1, Zusammenfassung; Spalte 14, Zeilen 33-63; Spalte 15, Zeilen 17-57; Anspruch 20), der üblicherweise unternommen wird um die Konsistenz der übermittelten Daten gegebenenfalls zu prüfen. Darauf kann keine erfinderische Tätigkeit basieren, da es für den Fachmann ein offensichtlicher Schritt wäre, die Lehren der Dokumenten D1 und D3 zu kombinieren um somit auf der im Anspruch 2 vorgeschlagenen Lösung zu kommen. Folglich liegt dem Gegenstand des unabhängigen Anspruchs 2 keine erfinderische Tätigkeit zugrunde.

2.2 Ansprüche 4 und 5:

Die abhängigen Ansprüche 4 und 5 enthalten keine Merkmale, die in Kombination mit den Merkmalen von Anspruch 2, auf den sie sich beziehen, die Erfordernisse des PCT in bezug auf erfinderische Tätigkeit erfüllen.

Beschreibungsseite 1a

Aus dem US-Patent US-PS 5,715,389 ist ein On-Line-Überwachungssystem für Computersysteme bekannt, bei dem die Zeit, welche für den Ablauf eine

5 Programms benötigt wird, ermittelt und mit einer vorgegebenen Zeit verglichen wird. Ein funktionaler Fehler bzw. mangelnde Verarbeitungseffizienz wird erkannt, wenn das überwachte Programm für seine Ausführung längere Zeit benötigt, als vorgesehen.

Neue Patentansprüche

1. Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen, wobei das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt dadurch gekennzeichnet, daß
- das aufrufende Programm über die zu übergebenden Parameter eine erste Checksumme bildet (Schritt 2),
 - diese erste Checksumme in einem dafür vorgesehenen Speicherbereich abgelegt wird,
 - das aufgerufene Programm vor seiner Ausführung über die erhaltenen Parameter eine zweite Checksumme (Schritt 5) bildet und auf Gleichheit mit der ersten Checksumme (Schritt 6) überprüft und
 - bei Ungleichheit der ersten und der zweiten Checksumme das Programm abgebrochen (Schritt 7) oder eine Fehlermeldung ausgegeben wird.
2. Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen, wobei das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt dadurch gekennzeichnet, daß bei Aufruf eines Unterprogramms ein Timer gestartet wird (Schritt 22), welcher die für die Ausführung des Programms benötigte Anzahl von Taktzyklen zählt und das Programm abbricht, wenn vor Beendigung des Unterprogramms die vorgegebene Anzahl der Taktzyklen überschritten wurde (Schritt 26).

- 2 -

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Speicherbereich zur Ablage der Checksumme ein RAM- oder Registerbereich ist.
- 5 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Rücksprungadressen der aufrufenden Funktion in einer Tabelle eingetragen werden und das aufgerufene Programm die vom aufrufenden Programm mitgeteilte Rücksprungadresse überprüft (Schritt 13), indem das Vorhandensein dieser Rücksprungadresse anhand der Tabelle überprüft wird.
- 10
5. Verfahren nach Anspruch 2 oder 4, dadurch gekennzeichnet, daß der Timerwert an bestimmten, vorgegebenen Stellen ausgelesen (Schritt 24) und mit einem ebenfalls vorgegebenen Zwischenwert verglichen wird (Schritt 25) und das Programm abgebrochen wird, wenn der vorgegebene Zwischenwert überschritten wurde (Schritt 26).
- 15

VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT
AM DEM GEBIET DES PATENTWESENS

PCT

INTERNATIONALER RECHERCHENBERICHT

(Artikel 18 sowie Regeln 43 und 44 PCT)

Aktenzeichen des Anmelders oder Anwalts K 51 755/7ch	WEITERES VORGEHEN siehe Mitteilung über die Übermittlung des internationalen Recherchenberichts (Formblatt PCT/ISA/220) sowie, soweit zutreffend, nachstehender Punkt 5	
Internationales Aktenzeichen PCT/EP 00/ 09131	Internationales Anmeldedatum (Tag/Monat/Jahr) 18/09/2000	(Frühestes) Prioritätsdatum (Tag/Monat/Jahr) 20/09/1999
Anmelder GIESECKE & DEVRIENT GMBH		

Dieser internationale Recherchenbericht wurde von der Internationalen Recherchenbehörde erstellt und wird dem Anmelder gemäß Artikel 18 übermittelt. Eine Kopie wird dem Internationalen Büro übermittelt.

Dieser internationale Recherchenbericht umfaßt insgesamt 3 Blätter.

☒ Darüber hinaus liegt ihm jeweils eine Kopie der in diesem Bericht genannten Unterlagen zum Stand der Technik bei.

1. Grundlage des Berichts

- a. Hinsichtlich der **Sprache** ist die internationale Recherche auf der Grundlage der internationalen Anmeldung in der Sprache durchgeführt worden, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.

☐ Die internationale Recherche ist auf der Grundlage einer bei der Behörde eingereichten Übersetzung der internationalen Anmeldung (Regel 23.1 b)) durchgeführt worden.

- b. Hinsichtlich der in der internationalen Anmeldung offenbarten **Nucleotid- und/oder Aminosäuresequenz** ist die internationale Recherche auf der Grundlage des Sequenzprotokolls durchgeführt worden, das

☐ in der internationalen Anmeldung in Schriftlicher Form enthalten ist.

☐ zusammen mit der internationalen Anmeldung in computerlesbarer Form eingereicht worden ist.

☐ bei der Behörde nachträglich in schriftlicher Form eingereicht worden ist.

☐ bei der Behörde nachträglich in computerlesbarer Form eingereicht worden ist.

☐ Die Erklärung, daß das nachträglich eingereichte schriftliche Sequenzprotokoll nicht über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht, wurde vorgelegt.

☐ Die Erklärung, daß die in computerlesbarer Form erfaßten Informationen dem schriftlichen Sequenzprotokoll entsprechen, wurde vorgelegt.

2. ☐ Bestimmte Ansprüche haben sich als nicht recherchierbar erwiesen (siehe Feld I).

3. ☐ Mangelnde Einheitlichkeit der Erfindung (siehe Feld II).

4. Hinsichtlich der **Bezeichnung der Erfindung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut von der Behörde wie folgt festgesetzt:

5. Hinsichtlich der **Zusammenfassung**

☒ wird der vom Anmelder eingereichte Wortlaut genehmigt.

☐ wurde der Wortlaut nach Regel 38.2b) in der in Feld III angegebenen Fassung von der Behörde festgesetzt. Der Anmelder kann der Behörde innerhalb eines Monats nach dem Datum der Absendung dieses internationalen Recherchenberichts eine Stellungnahme vorlegen.

6. Folgende Abbildung der **Zeichnungen** ist mit der Zusammenfassung zu veröffentlichen: Abb. Nr. 1

☐ wie vom Anmelder vorgeschlagen

☐ keine der Abb.

☒ weil der Anmelder selbst keine Abbildung vorgeschlagen hat.

☐ weil diese Abbildung die Erfindung besser kennzeichnet.

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
 IPK 7 G06F11/00 G06F11/28

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
 IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 651 111 A (REINIG AUGUST G ET AL) 22. Juli 1997 (1997-07-22) Zusammenfassung; Ansprüche 1-5 Spalte 12, Zeile 18 - Spalte 13, Zeile 8 ---	1,3-5
A	US 5 909 580 A (CRELIER REGIS ET AL) 1. Juni 1999 (1999-06-01) Zusammenfassung Spalte 12, Zeile 46 - Spalte 13, Zeile 24 Ansprüche 1-15 ---	1-5
A	US 5 768 591 A (ROBINSON JEFFREY I) 16. Juni 1998 (1998-06-16) Spalte 8, Zeile 38 - Zeile 62; Ansprüche 1-7 --- -/--	1-5

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

- *A* Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist
- *E* älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist
- *L* Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)
- *O* Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht
- *P* Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

1. Februar 2001

Absendedatum des internationalen Recherchenberichts

09/02/2001

Name und Postanschrift der Internationalen Recherchenbehörde
 Europäisches Patentamt, P.B. 5818 Patentlaan 2
 NL - 2280 HV Rijswijk
 Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
 Fax: (+31-70) 340-3016

Bevollmächtigter Bediensteter

Sarasua, L.

C.(Fortsetzung) ALS WESENTLICH ANGEKÜNDIGTE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 715 389 A (MORITA AKIO ET AL) 3. Februar 1998 (1998-02-03) Zusammenfassung; Ansprüche 1-4 ---	2
X	US 5 761 414 A (AKAISHI TSUYOSHI ET AL) 2. Juni 1998 (1998-06-02) Zusammenfassung; Ansprüche 1-6 -----	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

P 00/09131

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5651111	A	22-07-1997	EP	0686916 A	13-12-1995
US 5909580	A	01-06-1999	NONE		
US 5768591	A	16-06-1998	NONE		
US 5715389	A	03-02-1998	JP	2721294 B	04-03-1998
			JP	6231008 A	19-08-1994
US 5761414	A	02-06-1998	JP	9160807 A	20-06-1997
			FR	2742246 A	13-06-1997
			IT	MI962338 A	12-05-1998

101070444
Translation

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

77

Applicant's or agent's file reference K 51 755/7ch	FOR FURTHER ACTION See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)	
International application No. PCT/EP00/09131	International filing date (day/month/year) 18 September 2000 (18.09.00)	Priority date (day/month/year) 20 September 1999 (20.09.99)
International Patent Classification (IPC) or national classification and IPC G06F 11/00		
Applicant GIESECKE & DEVRIENT GMBH		

<p>1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.</p> <p>2. This REPORT consists of a total of <u>7</u> sheets, including this cover sheet.</p> <p><input checked="" type="checkbox"/> This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).</p> <p>These annexes consist of a total of <u>3</u> sheets.</p>
<p>3. This report contains indications relating to the following items:</p> <p>I <input checked="" type="checkbox"/> Basis of the report</p> <p>II <input type="checkbox"/> Priority</p> <p>III <input type="checkbox"/> Non-establishment of opinion with regard to novelty, inventive step and industrial applicability</p> <p>IV <input checked="" type="checkbox"/> Lack of unity of invention</p> <p>V <input checked="" type="checkbox"/> Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement</p> <p>VI <input type="checkbox"/> Certain documents cited</p> <p>VII <input type="checkbox"/> Certain defects in the international application</p> <p>VIII <input type="checkbox"/> Certain observations on the international application</p>

Date of submission of the demand 07 March 2001 (07.03.01)	Date of completion of this report 22 January 2002 (22.01.2002)
Name and mailing address of the IPEA/EP	Authorized officer
Facsimile No.	Telephone No.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP00/09131

I. Basis of the report

1. With regard to the elements of the international application:*

- ☐ the international application as originally filed
- ☒ the description:
 pages 1-7, as originally filed
 pages 1-7, filed with the demand
 pages 1a, filed with the letter of 26 November 2001 (26.11.2001)
- ☒ the claims:
 pages 1-5, as originally filed
 pages 1-5, as amended (together with any statement under Article 19)
 pages 1-5, filed with the demand
 pages 1-5, filed with the letter of 26 November 2001 (26.11.2001)
- ☒ the drawings:
 pages 1/2, 2/2, as originally filed
 pages 1/2, 2/2, filed with the demand
 pages 1/2, 2/2, filed with the letter of 26 November 2001 (26.11.2001)
- ☐ the sequence listing part of the description:
 pages 1-7, as originally filed
 pages 1-7, filed with the demand
 pages 1-7, filed with the letter of 26 November 2001 (26.11.2001)

2. With regard to the language, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.

These elements were available or furnished to this Authority in the following language English which is:

- ☐ the language of a translation furnished for the purposes of international search (under Rule 23.1(b)).
- ☐ the language of publication of the international application (under Rule 48.3(b)).
- ☐ the language of the translation furnished for the purposes of international preliminary examination (under Rule 55.2 and/or 55.3).

3. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

- ☐ contained in the international application in written form.
- ☐ filed together with the international application in computer readable form.
- ☐ furnished subsequently to this Authority in written form.
- ☐ furnished subsequently to this Authority in computer readable form.
- ☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
- ☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☐ The amendments have resulted in the cancellation of:

- ☐ the description, pages 1-7
- ☐ the claims, Nos. 1-5
- ☐ the drawings, sheets/fig 1/2, 2/2

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

* Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rule 70.16 and 70.17).

** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.

PCT/EP00/09131

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- ☐ restricted the claims.
- ☐ paid additional fees.
- ☐ paid additional fees under protest.
- ☐ neither restricted nor paid additional fees.

2. ☒ This Authority found that the requirement of unity of invention is not complied with and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

- ☐ complied with.
- ☒ not complied with for the following reasons:

SEE SEPARATE SHEET

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

- ☒ all parts.
- ☐ the parts relating to claims Nos. _____

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV.

1. Reference is made to the following documents:

D1 = US-A-5 651 111;

D2 = US-A-5 715 389;

D3 = US-A-5 761 414.

2. For the following reasons, the international application does not satisfy the requirements set forth in PCT Rule 13 regarding unity of invention:

The features common to Claims 1 and 2 are the following:

a process for protecting the integrity of program execution during subroutine calls, the program called carrying out a check of the data transmitted directly or indirectly by the calling program either prior to or during program execution.

Document D1 discloses all the common features of independent Claims 1 and 2 (see D1, abstract; column 14, lines 17-20 and 33-63; column 15, lines 17-57; Claim 20).

Although the process described in D1 has been developed for producing a software test system, it is also suitable for checking data that is transferred to a program called, the check being done by the called program itself (cf. PCT Guidelines, Part C, Chapter III-4.8).

Supplemental Box

(To be used when the space in any of the preceding boxes is not sufficient)

Continuation of: IV.

Consequently, the features common to independent Claims 1 and 2 are not novel. The required unity of invention (PCT Rule 13.1) is thus no longer present because no technical relationship according to PCT Rule 13.2 exists between the subjects of independent Claims 1 and 2 that is expressed in one or more of the same or corresponding special technical features.

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/EP 00/09131

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims	1-5	YES
	Claims		NO
Inventive step (IS)	Claims	1, 3-4	YES
	Claims	2, 4-5	NO
Industrial applicability (IA)	Claims	1-5	YES
	Claims		NO

2. Citations and explanations

1. First group: Claims 1, 3-4

The invention addresses the problem of making a process available for protecting program execution during subroutine calls, the program execution needing to be protected from unauthorized manipulation. This problem is solved by the process described in Claim 1. The process prevents unauthorized manipulation by requiring that a called program carry out a check of the data transmitted either directly or indirectly by the calling program prior to or during program execution. The check is done using a checksum. In particular, checksums are formed via the parameters to be passed before and after interchange and compared with each other. A disparity between the two checksums leads to program termination or an error message.

Document D1, which represents the closest prior art for Claim 1, describes a test process used in software development to automate testing of software modules. Although the process described in D1 mentions a check of the parameters passed under different routines, the disclosure of document D1

differs from the subject matter of Claim 1 in that the check is not done using checksums formed. D1 does not suggest that direction because it is concerned with a different problem (software testing, debugging, formal parameter check) than is the application (ensuring the integrity of program execution).

2. Second group: Claims 2, 4 and 5

2.1 Inventive step (PC Article 33(3)):

For the following reasons, the application does not satisfy the criteria set forth in PCT Article 33(3) regarding inventive step:

Claim 2:

Document D3, which is considered to be the closest prior art, discloses a process ensuring the integrity of program execution when subroutines are called (abstract) characterized in that, upon calling of a subroutine, a timer is set (abstract; Figure 1a; column 2, lines 17-21) that counts the number of pulse cycles required for program execution and aborts the program should the predetermined number of pulse cycles be exceeded prior to program termination (abstract).

Accordingly, the subject matter of independent Claim 2 differs from the process in D3 in that the program called carries out a check of the data transferred directly or indirectly by the calling program prior to or during program execution.

That feature represents a generally known process

step disclosed by the prior art (see for example D1, abstract; column 14, lines 33-63; column 15, lines 17-57; Claim 20) that is normally undertaken to check the consistency of the data transferred as necessary. That cannot substantiate an inventive step because it would be obvious to a person skilled in the art to combine the teaching of documents D1 and D3 and thereby to arrive at the solution proposed in Claim 2. Consequently, the subject matter of independent Claim 2 does not involve an inventive step.

2.2 Claims 4 and 5:

Dependent Claims 4 and 5 contain no features known in combination with the features of Claim 2, to which they refer, that satisfy the PCT requirements regarding inventive step.

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES
PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum
Internationales Büro



(43) Internationales Veröffentlichungsdatum
29. März 2001 (29.03.2001)

PCT

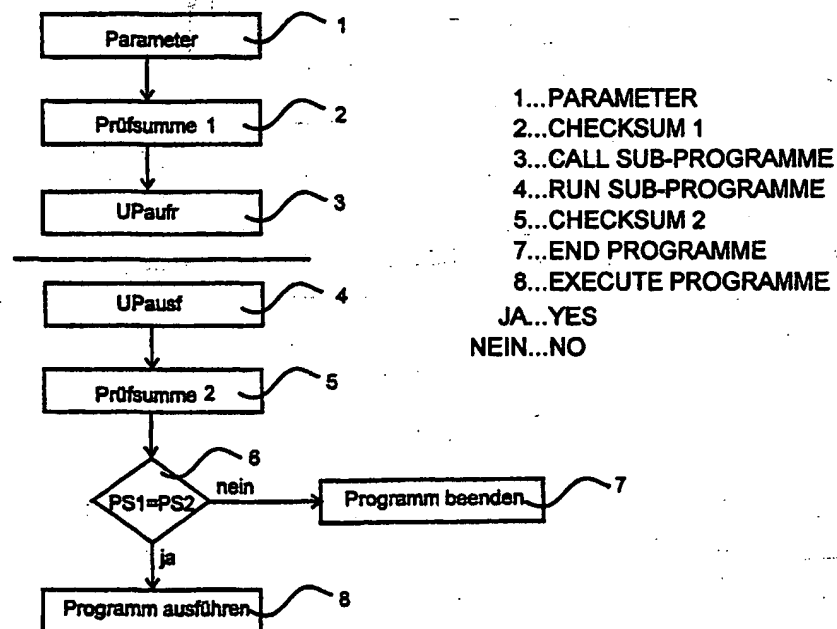
(10) Internationale Veröffentlichungsnummer
WO 01/22223 A1

- (51) Internationale Patentklassifikation⁷: G06F 11/00, 11/28
- (21) Internationales Aktenzeichen: PCT/EP00/09131
- (22) Internationales Anmeldedatum:
18. September 2000 (18.09.2000)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:
199 44 991.0 20. September 1999 (20.09.1999) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): GIESECKE & DEVRIENT GMBH [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): BALDISCHWEILER, Michael [DE/DE]; Hansjakobstrasse 99, 81825 München (DE).
- (74) Anwalt: KLUNKER, SCHMITT-NILSON, HIRSCH; Winzererstrasse 106, 80797 München (DE).
- (81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Bestimmungsstaaten (regional): ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),

[Fortsetzung auf der nächsten Seite]

(54) Title: METHOD FOR PROTECTING A PROGRAM FLOW

(54) Bezeichnung: VERFAHREN ZUR SICHERUNG EINES PROGRAMMABLAUFS



(57) Abstract: The invention relates to a method for protecting the program flow during sub-program calls. Known methods for protecting data contract the evaluation of data by specific interruption of the program, do not however offer any effective protection for modular programs, especially with regard to sub-program calls. According to the invention, the requested program therefor checks the data communicated directly or indirectly by the requesting program before or during the execution of the program.

[Fortsetzung auf der nächsten Seite]

WO 01/22223 A1



europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI-Patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Veröffentlicht:

— Mit internationalem Recherchenbericht.

— Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.

Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.

(57) Zusammenfassung: Die Erfindung betrifft ein Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen. Bekannte Verfahren zur Datensicherung wirken zwar einer Auswertung der Daten durch gezielte Programmunterbrechung entgegen, bieten jedoch keinen wirksamen Schutz bei modular aufgebauten Programmen, insbesondere beim Aufruf von Unterprogrammen. Gemäss der Erfindung führt deshalb das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten aus.

Verfahren zur Sicherung eines Programmablaufs

Die vorliegende Erfindung betrifft ein Verfahren zur Sicherung des Programmablaufs gemäß Anspruch 1.

Insbesondere bei sicherheitsrelevanten Anwendungen, beispielsweise im Bereich von IC-Karten ist es notwendig, den Programmablauf vor unerlaubten Manipulationen zu schützen. Zum Schutz geheimer Daten, beispielsweise geheimer Schlüsseldaten, ist es bekannt, die zu schützenden Daten verschlüsselt abzulegen, um ein Auslesen durch Unberechtigte zu verhindern.

Der Zugriff auf geheime Daten kann jedoch auch dadurch erfolgen, daß der Programmablauf gezielt unterbrochen wird, so daß Fehler in den Verschlüsselungsroutinen entstehen, aus denen nach mehrmaliger gezielter Unterbrechung auf die geheimen Daten rückgeschlossen werden kann.

Zur Vermeidung derartiger Angriffe ist es notwendig, Fehler oder Störungen des Programmablaufs sicher zu erkennen. Aus der deutschen Patentschrift DE 37 09 524 C2 ist ein Verfahren zur Überprüfung der Speicherzelleninhalte eines Programmspeichers in einem Rechner bekannt. Dort werden mehrere Prüfsummen abgespeichert, welche aus Speicherzelleninhalten von unterschiedlichen Adreß- und Datenspeicherbereichen gebildet werden. Die Prüfsummen werden zu Beginn und/oder während des Rechnerbetriebs ermittelt und mit der abgespeicherten Prüfsumme verglichen. Bei Feststellung einer Abweichung wird ein Fehlersignal ausgegeben.

Das aus der DE 37 09 524 C2 bekannte Verfahren eignet sich hauptsächlich dazu, die Richtigkeit von Daten, welche in einem Programm verwendet werden, zu überprüfen. Es wird außer Acht gelassen, daß auch bzw. insbe-

sondere bei Programmaufrufen, d.h. bei der Ausführung von Unter- oder Funktionsprogrammen eine Manipulation des Programmablaufs erfolgen kann.

- 5 Es ist deshalb Aufgabe der vorliegenden Erfindung, ein Verfahren anzugeben, das die sichere Überprüfung von modular aufgebauten Programmen, insbesondere bei Unterprogrammaufrufen, zuläßt.

- Gemäß der Erfindung wird diese Aufgabe gelöst, indem vom aufgerufenen
10 Programm eine Datenüberprüfung ausgeführt wird, welche den sicheren Übergang der vom aufrufenden Programm zu übergebenden Daten feststellt.

- Durch die Erfindung wird eine zusätzliche Sicherheit erreicht, die nicht nur
15 gewährleistet, daß einzelne Programmteile sicher und vollständig ausgeführt werden, sondern daß der gesamte Programmablauf ungestört und frei von Manipulationen ablaufen kann.

- Eine vorteilhafte Ausführungsform der Erfindung sieht vor, daß über die
20 vom aufrufenden Programm an das aufgerufene Programm übergebenen Parameter zunächst vom aufrufenden Programm eine Checksumme gebildet wird, welche in einem dafür vorgesehenen Speicherbereich abgelegt wird.
Nach Übergabe der Parameter wird auch vom aufgerufenen Programm über die erhaltenen Parameter eine Checksumme gebildet. Für den Fall, daß die
25 vom aufrufenden und aufgerufenen Programm gebildeten Checksummen unterschiedlich sind, wird das Programm abgebrochen.

Auf diese Weise kann sichergestellt werden, daß ein Funktionsprogramm, insbesondere ein Funktionsprogramm, welches sicherheitsrelevante Daten

abarbeitet, bereits zu Beginn auf Manipulationen hin untersucht wird, so daß der Start des aufgerufenen Programms mit fehlerhaften Parametern von vornherein verhindert werden kann und eine Auswertung der fehlerbehafteten Daten nicht ermöglicht wird.

5

Vorzugsweise wird der Speicherbereich, welcher zur Ablage der Checksumme vorgesehen ist, in einem RAM- oder Registerbereich angelegt.

Eine weitere oder alternative Ausführungsform zur Bildung der Checksumme über die zu übergebenden Parameter ergibt sich aus der Überprüfung der Rücksprungadressen. Dabei werden die Rücksprungadressen der aufrufenden Funktionen in einer Tabelle eingetragen und vom aufgerufenen Programm kann mittels dieser Tabelle überprüft werden, ob die vom aufrufenden Programm übermittelte Rücksprungadresse in der Tabelle vorhanden ist. Bei einer fehlerhaft mitgeteilten Rücksprungadresse kann das Programm unterbrochen werden.

Eine weitere alternative oder zusätzliche Sicherheitsüberprüfung kann erfolgen, indem bei Aufruf eines Unterprogramms bzw. eines Funktionsprogramms ein Timer gestartet wird. Dieser Timer zählt die Taktzyklen, welche für die Ausführung des Programms notwendig sind. Es wird dabei zunächst als Grenzwert für den Timer die für den regulären Unterprogrammablauf benötigte Anzahl der Taktzyklen als Grenzwert vorgegeben. Das Programm wird abgebrochen, wenn vor Beendigung des Unterprogramms die Anzahl der vorgegebenen Taktzyklen überschritten wurde.

In vorteilhafter Weise wird auch an bestimmten, vorgegebenen Stellen des Unterprogramms der Timerwert ausgelesen und mit ebenfalls vorgegebenen

Zwischenwerten verglichen. Auch in diesem Fall wird das Programm abgebrochen, wenn der vorgegebene Zwischenwert überschritten wurde.

Im folgenden wird die Erfindung anhand der Fig. 1 bis 3 näher erläutert.

5

Es zeigen:

Figur 1: Ablaufdiagramm für die Überprüfung mittels Prüfsumme

Figur 2: Ablauf für die Überprüfung mittels Rücksprungadressentabelle

10 Figur 3: Ablauf für die Überprüfung mittels Timer.

In Figur 1 ist der Ablauf eines Unterprogrammaufrufs, insbesondere eines Funktionsaufrufs beschrieben, wobei die Funktionsschritte 1 bis 3 das aufzurufende Programm betreffen und die Funktionsschritte 4 bis 8 die Auswertung des Unterprogramms betreffen.

Im aufzurufenden Programm werden zunächst in Schritt 1 die für die Ausführung des Unterprogramms notwendigen Parameter bereitgestellt. Für diese Parameter wird in Schritt 2 eine Prüfsumme gebildet, die im einfachsten Fall aus einem Parity-check bestehen kann. Im weiteren sind selbstverständlich die gängigen Verfahren zur Prüfsummenbildung, z.B. CRC (Cyclical Redundancy Check) oder EDC einsetzbar. Die so ermittelte Prüfsumme (Checksumme) wird in einen dafür vorgesehenen Speicherbereich eingeschrieben. Bei diesem Speicherbereich kann es sich um einen flüchtigen Speicher (RAM) oder auch um einen nichtflüchtigen, wiederbeschreibbaren Speicher (z.B. EEPROM) handeln.

In Anschluß an die Bildung und Abspeicherung der Prüfsumme 1 erfolgt der Unterprogrammaufruf in Schritt 3. Schritt 4 stellt den Beginn der Ausführ-

rung des Unterprogramms dar. In diesem Unterprogramm wird zunächst die Prüfsumme 2 über die übergebenen Parameter gebildet. Diese Prüfsumme wird mit dem gleichen Verfahren gebildet, mit dem auch die Prüfsumme 1 im aufrufenden Programm ermittelt wurde.

5

Als nächstes erfolgt in Schritt 6 eine Überprüfung der Prüfsummen PS1 und PS2 auf Gleichheit. Wird in diesem Schritt 6 festgestellt, daß die beiden Prüfsummen ungleich sind, kann davon ausgegangen werden, daß bei der Übergabe der Programmparameter ein Fehler aufgetreten ist, welcher ein Hinweis auf eine beabsichtigte Störung mit dem Ziel, Geheimdaten zu ermitteln, sein kann. Als Maßnahme kann in Schritt 7 das Programm beendet werden oder es werden entsprechende alternative Maßnahmen getroffen, beispielsweise eine Fehlermeldung an das Hauptprogramm.

10

15 Wird in Schritt 6 festgestellt, daß die Prüfsummen PS1 und PS2 gleich sind, wird mit der eigentlichen Funktionsausführung begonnen.

20

Die Figur 2 zeigt eine Möglichkeit der Programmsicherung durch Überprüfen der Rücksprungadressen. Rücksprungadressen werden beim Funktionsaufruf per Hardware auf den Stack gelegt. Im vorliegenden Fall werden also im Schritt 11 beim Unterprogrammaufruf, ebenfalls die Informationen vom aufrufenden Programm (z.B. Rücksprungadressen) an das Unterprogramm übergeben. Gemäß der Erfindung werden die Rücksprungadressen in einer Tabelle 17 verwaltet und bei der Ausführung des Unterprogramms werden
25 zunächst in Schritt 12 die Rücksprungadressen - soweit sie im RAM abgelegt sind - auf Konsistenz hin untersucht, um sie in Schritt 13 anhand der Tabelle 17 zu überprüfen. Wenn in Schritt 14 festgestellt wurde, daß die übergebene Rücksprungadresse nicht in der Tabelle vorhanden ist, wird mit Schritt 15

das Programm beendet, andernfalls wird in Schritt 16 mit der Ausführung des Funktionsprogramms begonnen.

Die Figur 3 zeigt eine Ausführungsform, bei der der richtige Programmablauf bzw. der ungestörte Programmablauf mittels eines Timers überprüft wird. Unmittelbar nach dem Start des Unterprogramms in Schritt 21 wird in Schritt 22 ein Timer gestartet. Dieser Timer ist ausgelegt, die Zeit zu messen bzw. die Taktzyklen zu zählen, welche für die Ausführung des Unterprogramms benötigt werden. Im Anschluß an den Start des Timers in Schritt 22 wird mit Schritt 23 die Funktion des Unterprogramms ausgeführt und nach Beendigung der Funktion wird in Schritt 24 der Timer gestoppt. In Schritt 25 wird überprüft, ob die Anzahl der Taktzyklen, welche für die Ausführung des Funktionsprogramms benötigt wurden, mit der vorgegebenen Anzahl von Taktzyklen übereinstimmt. Für den Fall, daß keine Übereinstimmung besteht, wird das Programm mit Schritt 26 beendet. Im anderen Fall wird in Schritt 27 mit der Programmausführung fortgefahren, beispielsweise indem zum Hauptprogramm zurückgesprungen wird.

In der Figur 3 ist dargestellt, daß der Timer nach Ablauf der Funktion bzw. des Funktionsprogramms gestoppt und überprüft wird. In der Praxis kann die Sicherheit erhöht werden, indem bestimmte Stellen im Funktionsprogramm vorgesehen werden, an denen der Timer zusätzlich überprüft wird. Damit kann gegebenenfalls verhindert werden, daß das Funktionsprogramm trotz eines Fehlers oder Angriffs weitgehend ausgeführt wird.

Alternativ kann auch vorgesehen werden, daß der Timerwert nach dem Start kontinuierlich mit einem Grenzwert verglichen wird und das Programm abgebrochen wird, wenn dieser Grenzwert erreicht bzw. überschritten wurde.

Die einzelnen Ausführungsbeispiele nach den Figuren 1 bis 3 wurden als eigenständige, alternative Maßnahmen dargestellt. Die Sicherheit kann erhöht werden, indem die Ausführungsbeispiele kombiniert werden. Größte Sicherheit bildet die parallele Überprüfung mittels Prüfsumme, Rücksprungadressenprüfung und Timerüberprüfung.

5

Neue Patentansprüche

1. Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen, wobei das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt dadurch gekennzeichnet, daß
- das aufrufende Programm über die zu übergebenden Parameter eine erste Checksumme bildet,
 - diese erste Checksumme in einem dafür vorgesehenen Speicherbereich abgelegt wird,
 - das aufgerufene Programm vor seiner Ausführung über die erhaltenen Parameter eine zweite Checksumme bildet und auf Gleichheit mit der ersten Checksumme überprüft und
 - bei Ungleichheit der ersten und der zweiten Checksumme das Programm abgebrochen oder eine Fehlermeldung ausgegeben wird.
2. Verfahren zur Sicherung des Programmablaufs beim Aufruf von Unterprogrammen, wobei das aufgerufene Programm vor bzw. während der Programmausführung eine Überprüfung der vom aufrufenden Programm direkt oder indirekt übermittelten Daten ausführt dadurch gekennzeichnet, daß bei Aufruf eines Unterprogramms ein Timer gestartet wird, welcher die für die Ausführung des Programms benötigte Anzahl von Taktzyklen zählt und das Programm abbricht, wenn vor Beendigung des Unterprogramms die vorgegebene Anzahl der Taktzyklen überschritten wurde.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß der Speicherbereich zur Ablage der Checksumme ein RAM- oder Registerbereich ist.
- 5 4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Rücksprungadressen der aufrufenden Funktion in einer Tabelle eingetragen werden und das aufgerufene Programm die vom aufrufenden Programm mitgeteilte Rücksprungadresse überprüft, indem das Vorhandensein dieser Rücksprungadresse anhand der Tabelle überprüft wird.
10
5. Verfahren nach einem der Ansprüche 2 - 4, dadurch gekennzeichnet, daß der Timerwert an bestimmten, vorgegebenen Stellen ausgelesen und mit einem ebenfalls vorgegebenen Zwischenwert verglichen wird und das Programm abgebrochen wird, wenn der vorgegebene Zwischenwert überschritten wurde.
15

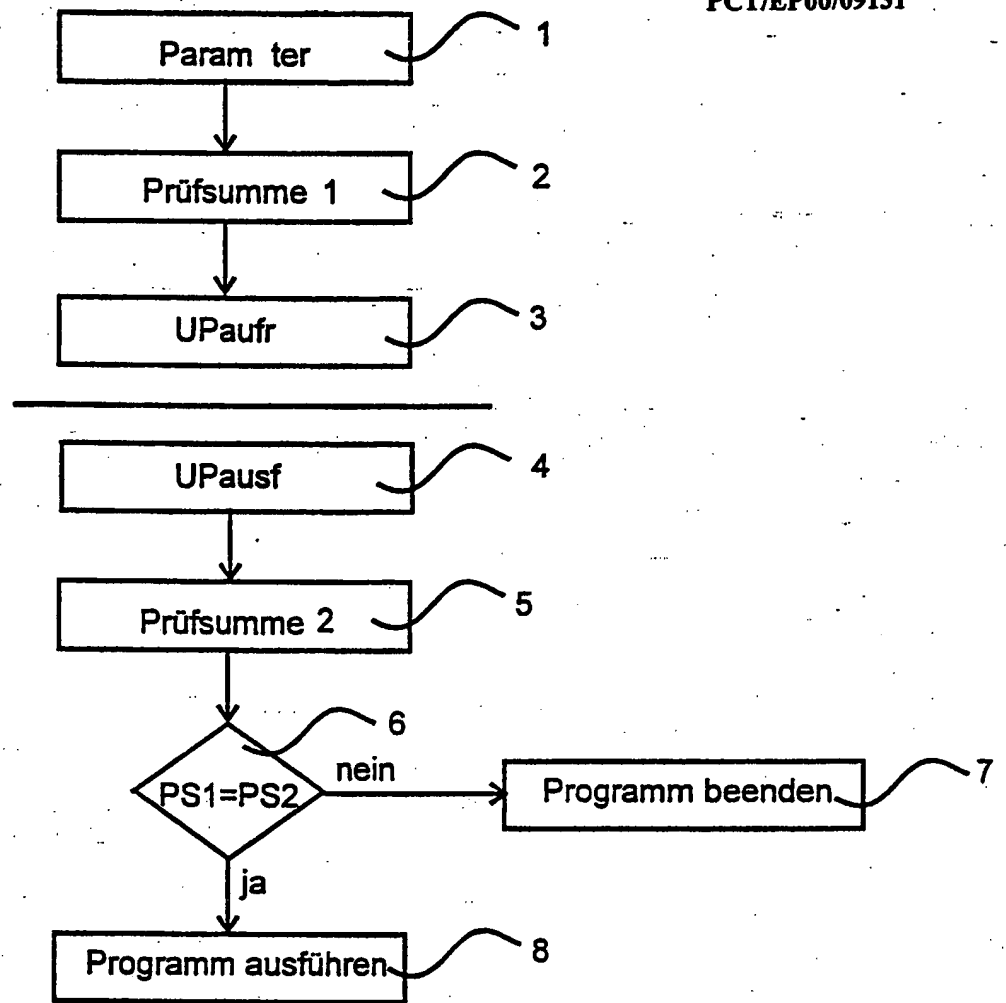


Fig. 1

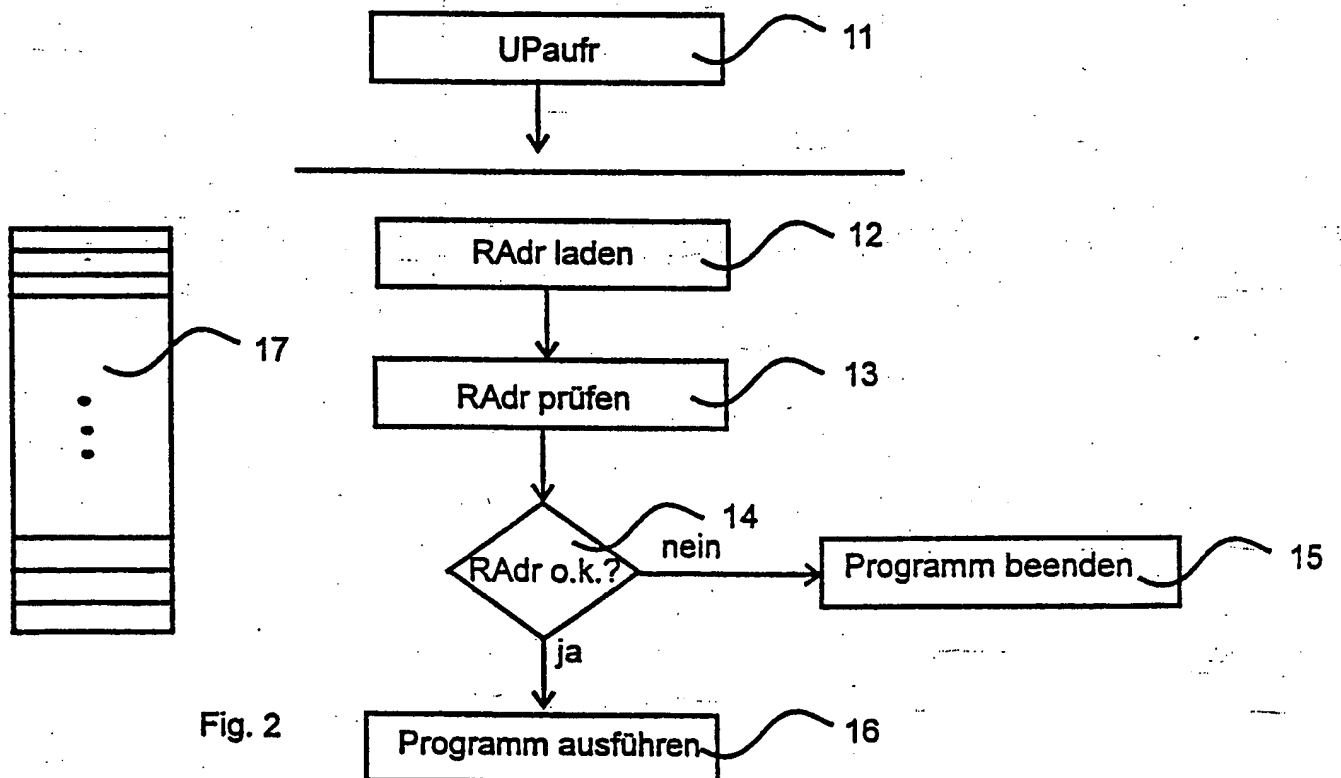


Fig. 2

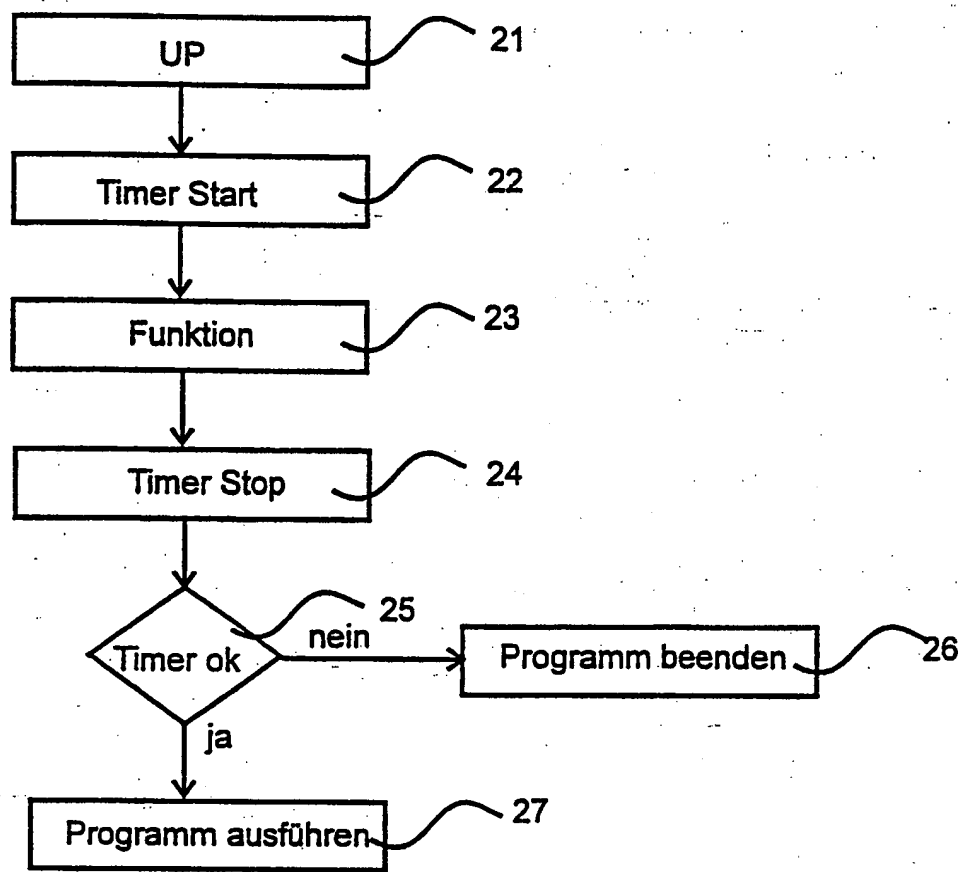


Fig. 3

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/09131

A. CLASSIFICATION OF SUBJECT MATTER

IPC 7 G06F11/00 G06F11/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 651 111 A (REINIG AUGUST G ET AL) 22 July 1997 (1997-07-22) abstract; claims 1-5 column 12, line 18 -column 13, line 8	1,3-5
A	US 5 909 580 A (CRELIER REGIS ET AL) 1 June 1999 (1999-06-01) abstract column 12, line 46 -column 13, line 24 claims 1-15	1-5
A	US 5 768 591 A (ROBINSON JEFFREY I) 16 June 1998 (1998-06-16) column 8, line 38 - line 62; claims 1-7	1-5
X	US 5 715 389 A (MORITA AKIO ET AL) 3 February 1998 (1998-02-03) abstract; claims 1-4	2
-/-		

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

X document of particular relevance: the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance: the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

& document member of the same patent family

Date of the actual completion of the international search

1 February 2001

Date of mailing of the international search report

09/02/2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sarasua, L.

INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/09131

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>US 5.761.414 A (AKAISHI TSUYOSHI ET AL) 2 June 1998 (1998-06-02) abstract; claims 1-6</p>	2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/09131

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 5651111	A	22-07-1997	EP 0686916 A	13-12-1995
US 5909580	A	01-06-1999	NONE	
US 5768591	A	16-06-1998	NONE	
US 5715389	A	03-02-1998	JP 2721294 B	04-03-1998
			JP 6231008 A	19-08-1994
US 5761414	A	02-06-1998	JP 9160807 A	20-06-1997
			FR 2742246 A	13-06-1997
			IT MI962338 A	12-05-1998

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 G06F11/00 G06F11/28

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 G06F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 651 111 A (REINIG AUGUST G ET AL) 22. Juli 1997 (1997-07-22) Zusammenfassung; Ansprüche 1-5 Spalte 12, Zeile 18 - Spalte 13, Zeile 8	1,3-5
A	US 5 909 580 A (CRELIER REGIS ET AL) 1. Juni 1999 (1999-06-01) Zusammenfassung Spalte 12, Zeile 46 - Spalte 13, Zeile 24 Ansprüche 1-15	1-5
A	US 5 768 591 A (ROBINSON JEFFREY I) 16. Juni 1998 (1998-06-16) Spalte 8, Zeile 38 - Zeile 62; Ansprüche 1-7	1-5
	-/-	

☒ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

* Besondere Kategorien von angegebenen Veröffentlichungen :

A Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

E älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

L Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

O Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

P Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

T Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

X Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfindertischer Tätigkeit beruhend betrachtet werden

Y Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindertischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

Z Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

1. Februar 2001

Absenddatum des internationalen Recherchenberichts

09/02/2001

Name und Postanschrift der internationalen Recherchenbehörde

Europäisches Patentamt, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

-Bevollmächtigter Bediensteter

Sarasua, L.

C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US-5 715 389 A (MORITA AKIO ET AL) 3. Februar 1998 (1998-02-03) Zusammenfassung; Ansprüche 1-4	2
X	US 5 761 414 A (AKAISHI TSUYOSHI ET AL) 2. Juni 1998 (1998-06-02) Zusammenfassung; Ansprüche 1-6	2

INTERNATIONALER RESEARCHENBERICHT

Angaben zu Veröffentlichung, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/09131

Im Recherchenbericht angeführtes Patentdokument		Datum der Veröffentlichung	Mitglied(er) der Patentfamilie		Datum der Veröffentlichung
US 5651111	A	22-07-1997	EP	0686916 A	13-12-1995
US 5909580	A	01-06-1999	KEINE		
US 5768591	A	16-06-1998	KEINE		
US 5715389	A	03-02-1998	JP	2721294 B	04-03-1998
			JP	6231008 A	19-08-1994
US 5761414	A	02-06-1998	JP	9160807 A	20-06-1997
			FR	2742246 A	13-06-1997
			IT	MI962338 A	12-05-1998